عنوان پست سازمانی: کارشناس مسئول حفاظت رایانه و فناوری اطلاعات

عنوان پست سرپرست مستقیم: رئیس اداره حفاظت فناوری اطلاعات / مدیر حراست

جایگاه پست: ستاد ■ نام واحد ستادی: حوزه ریاست دانشگاه

واحدهای محیطی □ نام واحد محیطی: .....

نام واحد/ بخش سازمانی: مدیریت حراست

	شرح وظایف اجرایی / عملیاتی متصدی پست سازمانی
۱	استقرار سیستم یکپارچه مدیریت کاربران
۲	حصول اطمینان از صحت انتساب نقش متناسب با هویت و وظایف مبتنی بر قلمرو و مجوزهای صادره
۳	اِعمال چرخه حیات هویت در سامانه‌ها از تخصیص تا حذف و ایجاد فرایندهای متناسب با آن
۴	تدوین و ارزیابی کنترل‌های امنیتی بر روی داده‌ها و اطلاعات حراست
۵	پیاده سازی، اجرا و پشتیبانی سامانه اختصاصی سیستم یکپارچه اتوماسیون اداری محرمانه، پرسنلی و خبر در محیط حراست و مدیریت دیجیتالی کردن مستندات بر اساس استانداردهای ابلاغی نظیر الکترونیکی نمودن پرونده ها
۶	تحلیل تهدیدات و انجام کنترل‌های امنیتی لازم از طریق بهره‌گیری از فناوری‌های مرتبط در گستره کسب و کار سازمان
۷	انجام بازر سی‌های دوره‌ای از حرا ست‌های تابعه به منظور اطمینان از انطباق و ضعیت موجود با سیا ست‌ها و خط م شی‌های امنیتی حراست
۸	پیگیری ت شکیل کمیته برون سپاری و ح ضور در جل سات مرتبط با حوزه فناوری اطلاعات در را ستای صیانت از اطلاعات سازمان
۹	پیگیری تشکیل کمیته مدیریت امنیت اطلاعات و عضویت نماینده حفاظت فناوری اطلاعات در کمیته و حضور در شورای راهبردی فناوری اطلاعات سازمان
۱۰	ارزیابی و نظارت بر سطوح مختلف سیستمی و فرآیندی سازمان (اعم از حراست و فناوری اطلاعات)
۱۱	انجام سایر امور محوله به دستور مافوق طبق قوانین و مقررات
	برنامه‌ریزی / سازماندهی / نظارت / هماهنگی
۱	نظارت بر حسن اجرای مصوبات کمیته‌های مرتبط با شرح وظایف شش‌گانه حوزه حفاظت فناوری اطلاعات
۲	نظارت و پیگیری ایجاد فرایند اصالت‌سنجی کاربران در سامانه‌ها
۳	نظارت بر تهیه مقررات و دستورالعمل‌های حفاظتی و امنیتی در تولید، نگهداری، گردش و دسترسی به اطلاعات در سیستم‌های اطلاعاتی
۴	نظارت بر ایجاد پایگاه داده امن منطبق بر استانداردها و چارچوب‌های پذیرفته شده
۵	نظارت بر تدوین و ا ستقرار معماری و طبقه بندی اطلاعات به منظور مقابله با مخاطرات مترتب؛ نظیر ن شت اطلاعات، تخریب اطلاعات و دسترسی‌های غیر مجاز در راستای حفاظت از کسب و کار دستگاه
۶	م ستند سازی فرایندها و دارایی‌های اطلاعاتی و به روز ر سانی دوره‌ای آنها منطبق بر ا ستانداردهای مربوطه از جمله نظارت بر تهیه شناسنامه الکترونیکی از شبکه، سخت‌افزار و نرم‌افزار
۷	نظارت، پیگیری و ارزیابی مستمر بر چرخه حیات داده به منظور صیانت از اطلاعات دستگاه از جمله نظارت بر تهیه نسخ پشتیبان از بانک‌های اطلاعاتی به صورت منظم و دوره‌ای و نگهداری آن در فضای امن متناسب با استانداردها

۸	نظارت بر حسن اجرای الزامات امنیتی حوزه فناوری اطلاعات شامل اخذ گواهینامه‌های امنیتی نرم‌افزارها، سرویس‌ها و سامانه‌ها از مراجع ذی صلاح قبل از انعقاد قرارداد
۹	نظارت بر طراحی، توسعه و استقرار امن و یکپارچه نرم‌افزارها، سرویس‌ها و سامانه‌های حراست و مدیریت چرخه حیات آنها منطبق بر استانداردها و چارچوب‌های پذیرفته شده
۱۰	نظارت و ارزیابی انجام آزمون‌های امنیتی حوزه فناوری اطلاعات در جهت شناسایی آسیب‌پذیری‌های نرم‌افزار، زیر ساخت و سامانه‌ها
۱۱	نظارت بر اجرای کنترل‌های حفاظتی مرتبط با سازوکارهای تبادل اطلاعات سیستمی بین دستگاه و شرکت‌های طرف قرارداد
۱۲	نظارت بر تدوین سیاست‌ها و اِعمال محدودیت‌های مورد نیاز در نصب و اجرای نرم‌افزارها، سرویس‌ها و کارکردهای غیر سازمانی شامل پیام رسان‌ها یا شبکه‌های اجتماعی
۱۳	نظارت بر بلوغ حفاظتی و امنیتی ارکان فناوری اطلاعات دستگاه با محوریت متدلوژی و استانداردهای پذیرفته شده
۱۴	نظارت بر تدوین راهبرد مدیریت آسیب‌پذیری، تهدید و رویداد در حوزه فناوری اطلاعات سازمان؛ شامل پیگیری و نظارت بر پیاده سازی مرکز عملیات امنیت
۱۵	نظارت بر پایش، کنترل و کاهش آسیب‌پذیری‌ها و تهدیدات بر اساس چارچوب‌ها و استانداردهای مرتبط
۱۶	نظارت بر ایجاد فرآیند مستمر ارزیابی مخاطرات حوزه فناوری اطلاعات؛ شامل پیگیری و نظارت بر انجام دوره‌ای آزمون سنجش نفوذپذیری
۱۷	نظارت بر حُسن اجرای میز خدمت سازمان در حوزه امنیت اطلاعات و سایر زیرمولفه‌های سرویس‌های فناوری اطلاعات و اخذ گزارشات موردی از آن
۱۸	نظارت بر تفکیک شبکه‌های رایانه‌ای و اِعمال کنترل‌های امنیتی در راستای پیشگیری از دسترسی‌های غیرمجاز به منابع شبکه شامل پورت‌های فیزیکی و منطقی سرورها، کلاینت‌ها و تجهیزات مربوطه
۱۹	نظارت بر پیاده سازی، توسعه و پشتیبانی سامانه‌های هوشمند حفاظتی اعم از سامانه‌های پایش تصویری با محوریت تأمین امنیت فناوری اطلاعات
۲۰	نظارت بر راه‌اندازی و استانداردسازی مراکز داده دستگاه و تعیین ضوابط کلی حفاظتی آن بر اساس زیرمولفه‌های مرتبط با حوزه امنیت فناوری اطلاعات
۲۱	نظارت بر پیاده‌سازی استانداردهای معماری شبکه در راستای تامین امنیت و پوشش نقاط نفوذ
۲۲	نظارت بر حسن اجرای ضوابط حفاظتی در خصوص نقل و انتقال و امحاء سخت‌افزاری و نرم‌افزاری تجهیزات دستگاه
۲۳	نظارت بر حسن اجرای ضوابط حفاظتی در خصوص نصب و اتصال هر نوع تجهیزات ارتباطی و الکترونیکی اعم از کارت شبکه بی‌سیم، مودم، تلفن همراه، روتر در کلیه مبادی مرتبط با شبکه دستگاه
آموزش/پژوهش/نوآوری/ بهبود کیفیت	
۱	حضور در دوره های آموزشی درون و برون‌سازمانی و پیگیری اجرای آن از واحدهای مرتبط ذیصلاح